FortiCloud Administration Guide

VERSION 3.3.0

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

Thursday, July 26, 2018

FortiCloud Administration Guide Version 3.3.0

32-330-480481-20180726

TABLE OF CONTENTS

Introduction

This guide provides information about the FortiCloud service.

It is divided into three sections:

- The **FortiCloud User Guide**, a list of pages and features available in the FortiCloud web interface,
- the **Frequently Asked Questions**, a collection of general and specific information about the service,
- and the **FortiCloud Cookbook**, a series of short-form tutorials that teach how to perform tasks in FortiCloud, ranging from basic to complex.

Overview of FortiCloud

FortiCloud is a hosted security and wireless infrastructure management solution and log retention service for FortiGate, FortiWiFi, and FortiAP devices.

It gives you centralized reporting, traffic analysis, configuration management, and log retention without the need for additional hardware and software, with the following feature set:

- Simple provisioning of large scale security networks
- Configuration and device management from a single pane of glass
- Hosted log retention and cloud-based storage
- Built-in protection from APTs with FortiGuard sandboxing technology
- Instant security intelligence and analytics with FortiView
- Exceptional network visibility with FortiCloud reporting
- FortiCloud transport security and service availability

FortiCloud also integrates these other Fortinet services: **FortiCloud Sandbox**, and **FortiDeploy**.

FortiCloud Sandbox

FortiCloud Sandbox is a service that uploads and analyzes files marked as suspicious by the FortiGate AntiVirus.

In a proxy-based antivirus profile on a FortiGate, the administrator selects Inspect Suspicious Files with FortiGuard Analytics to enable a FortiGate unit to upload suspicious files to FortiGuard for analysis. Once uploaded, the file will be executed and the resulting behavior analyzed for risk. If the file exhibits risky behavior or is found to contain a virus, a new virus signature is created and added to the FortiGuard antivirus signature database. The next time the FortiGate unit updates its antivirus database it will have the new signature.

FortiGuard Labs considers a file suspicious if it exhibits some unusual behavior, yet does not contain a known virus (the behaviors that FortiCloud Analytics considers suspicious will change depending on the current threat climate and other factors).

The FortiCloud console enables administrators to view the status of any suspicious files uploaded: Pending, Clean, Malware, or Unknown. The console also provides data on time, user, and location of the infected file for forensic analysis. Sandboxing is available in both Free and Paid FortiCloud subscriptions.

FortiDeploy

FortiDeploy is a product built into FortiCloud as a feature, for one-touch provisioning when devices are deployed, locally or remotely. FortiDeploy provides deployment for FortiAPs into a Cloud AP Network, and automatic connection of FortiGates to be managed by FortiCloud or a FortiManager unit.

At time of purchase, you can order a FortiDeploy SKU in addition to your FortiCloud subscription.

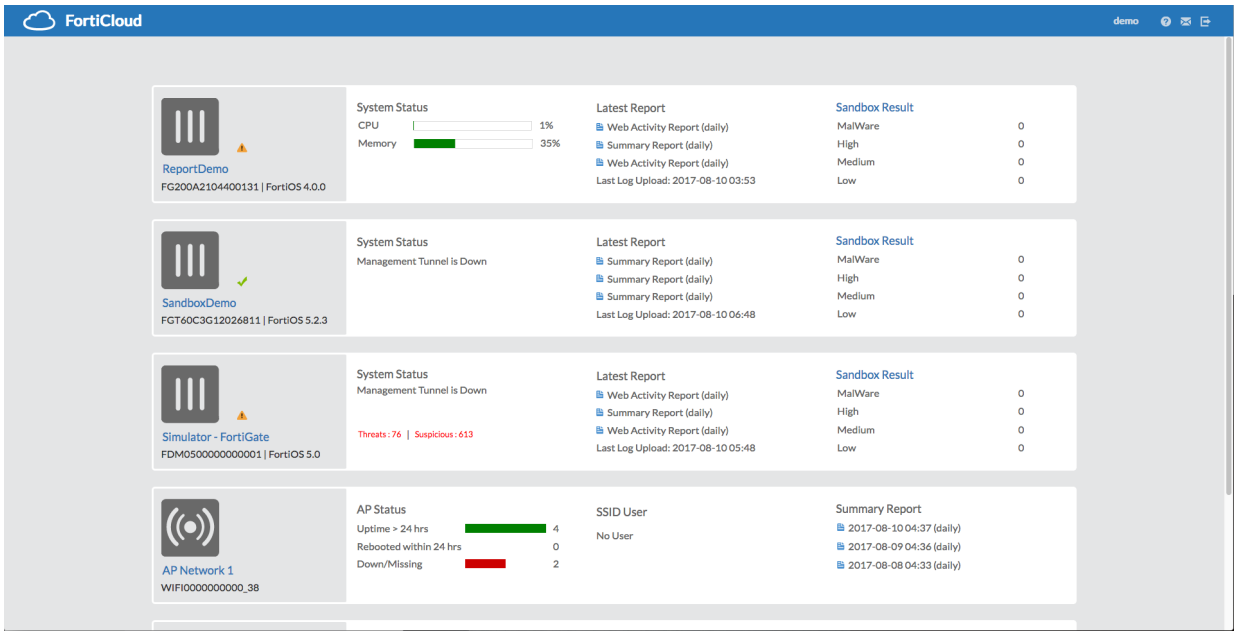
When you visit forticloud.com and enter the Bulk FortiCloud Key, you will see a list of serial numbers from the order that contained the FortiDeploy SKU. Once you confirm that the devices are connected, you can perform basic configuration on the devices remotely, such as sending a FortiManager IP to all remote FortiGate devices, so they can be managed remotely.

FortiDeploy Support starts the moment you send an email to cs@fortinet.com, which can also be contacted if you have already purchased a FortiCloud subscription and would like to purchase FortiDeploy to add to your existing subscription.

FortiCloud user guide

Home page

You will see the **Home** page when you first open the FortiCloud interface.



On the Home page is a list of Fortinet devices connected to the FortiCloud service.

New devices can be added by selecting Add Device above the list, and entering a FortiCloud Key.

Each Device displays:

- the Model/Serial Number
- the Fortinet Product (FortiGate, FortiAP, etc)
- if the device is connected through a Management Tunnel
- the last compiled report and the last log uploaded
- what percentage of the FortiCloud Quota has been filled (and a Manage Quota button, that allows you to delete old logs and make space on the server)
- a yellow Warning symbol, or a green Check symbol, to show subscription status.

Next to some device icons will be a gear icon, allowing you to delete/rename/configure devices.

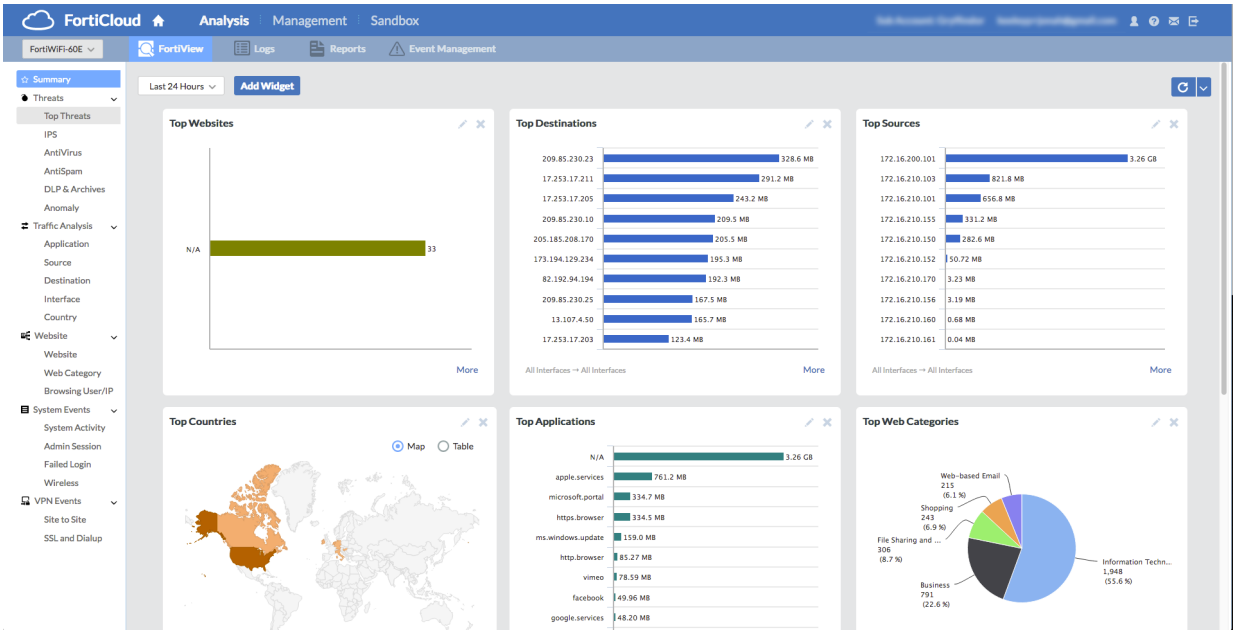
Click on a device icon to go to the FortiCloud Dashboard for that device.

Analysis pages

The **Analysis** pages provide tools for monitoring and logging your device's traffic, providing you centralized oversight of traffic and security events.

FortiView: Summary

The default **FortiView** page is the **Summary** view, general overview of what is happening with your device, using many Widgets.



Each Widget is a customizable box, showing certain information about the device.

- You can click on a Widget title and drag it to move it around.
- You can customize any Widget by selecting the Pencil icon.
- You can delete a Widget by selecting the X icon.
- You can set the refresh rate of Widgets by selecting the Refresh icon in the upper right.

New Widgets can be added by clicking the “Add Widget” button in the upper left.

Widget list

All of the Widgets are listed below.

Threats

- **Top Threats** displays which Threats are triggering the most detection events on the network. (One or more of the following must be configured on the device: IPS, AntiVirus, AntiSpam, DLP, Anomaly Detection.)
- **Top Spam** displays which Sources are sending the most Spam email into the network. (AntiSpam must be configured on the device.)
- **Top Viruses** counts the viruses most frequently found by the device's AntiVirus. (AntiVirus must be configured on the device.)
- **Top Applications by Threat Score** compares which Applications have the most traffic compared to their Threat Score, based on the device's Application Control settings. (Application Control must be configured on the device.)
- **Top Attacks** counts the attacks most frequently prevented by the device's IPS. (IPS must be configured on the device.)
- **Top DLP By Rules** counts the DLP events detected by the device, sorted by DLP rule. (DLP must be configured on the device.)

Traffic Analysis

- **Top Applications** compares which Applications are most frequently used, based on the device's Application Control settings. (Application Control must be configured on the device.)
- **Top Application Categories** compares which Application Categories are most frequently used, based on the device's Application Control settings. (Application Control must be configured on the device.)
- **Top Sources** displays which Sources have the most traffic from or to the device.
- **Top Destinations** displays which Destinations have the most traffic from or to the device.
- **Top Protocols** compares the traffic volume that has passed through a certain interface, based on which protocol it uses (http, https, dns, tcp, udp, other).
- **Top Countries** displays which Countries have the most traffic from or to the device.
- **Traffic History** is a chart that displays the volume of Incoming and Outgoing traffic over time.

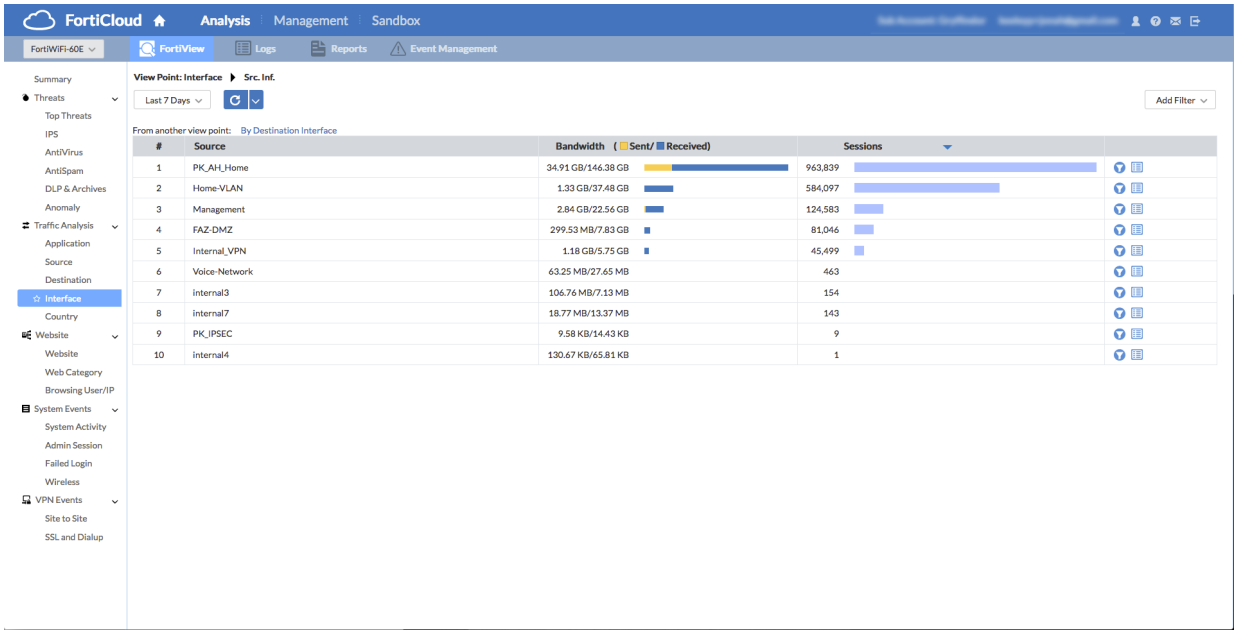
Websites

- **Top Websites** compares which websites are most frequently visited. You can click on a category to see which websites in that category are being visited. (Web Filtering must be configured on the device.)
- **Top Web Categories** compares which Web Filtering Categories are most frequently used, based on the device's Web Filtering settings. (Web Filtering must be configured on the device.)
- **Top Users/IP by Browsing Time In Seconds** compares which IPS are most frequently visited by which users in the greatest ratio. You can click on a user to see which IPs they are visiting. (Web Filtering must be configured on the device.)

FortiView: Sections

The various **FortiView** subpages offer log information, reformatted into easily navigable charts, in a similar style as the FortiGate's FortiView pages. Each page is styled differently to suit the information structure.

The below screenshot shows the **Interface** subpage, showing Source Interfaces charted by traffic volume.



The menu to the right of the subpage list allows you to select a time period to view:

- Last 60 Minutes
- Last 24 Hours
- Last 7 Days
- Last 30 Days
- Specified Time Period

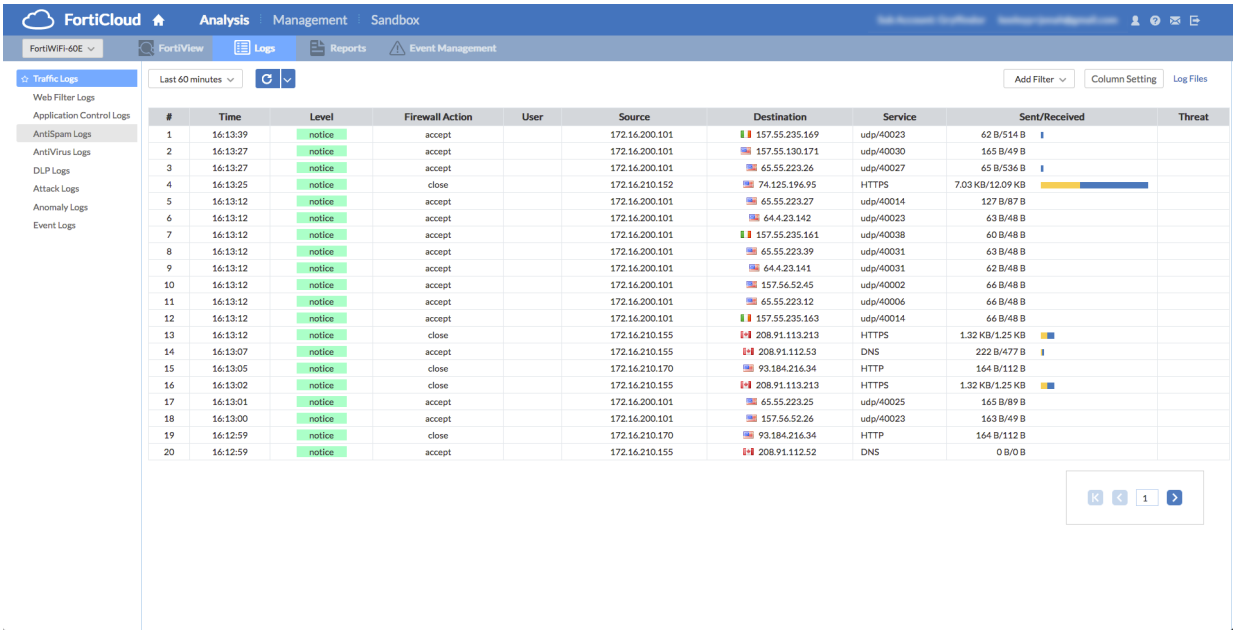
You can set the refresh rate of the chart by selecting the Refresh icon to the right of the time period.

By selecting **Add Filter** in the upper right, you can filter the chart by various factors; individual chart entries may also allow you to filter by that entry's data by selecting a Filter icon on the right, or drill down to see all related log data (e.g. all log data through that interface.)

Logs

The **Log** pages offer more detailed log information, access to individual log data, and downloadable log files.

The below screenshot shows the **Traffic Logs**subpage, showing traffic log data collected by the device.



#	Time	Level	Firewall Action	User	Source	Destination	Service	Sent/Received	Threat
1	16:13:39	notice	accept		172.16.200.101	157.55.235.169	udp/40023	62 B/514 B	
2	16:13:27	notice	accept		172.16.200.101	157.55.130.171	udp/40030	165 B/49 B	
3	16:13:27	notice	accept		172.16.200.101	65.55.223.26	udp/40027	65 B/536 B	
4	16:13:25	notice	close		172.16.210.152	74.125.196.95	HTTPS	7.03 KB/12.09 KB	
5	16:13:12	notice	accept		172.16.200.101	65.55.223.27	udp/40014	127 B/87 B	
6	16:13:12	notice	accept		172.16.200.101	64.4.23.142	udp/40023	63 B/48 B	
7	16:13:12	notice	accept		172.16.200.101	157.55.235.161	udp/40038	60 B/48 B	
8	16:13:12	notice	accept		172.16.200.101	65.55.223.39	udp/40031	63 B/48 B	
9	16:13:12	notice	accept		172.16.200.101	64.4.23.141	udp/40031	62 B/48 B	
10	16:13:12	notice	accept		172.16.200.101	157.56.52.45	udp/40002	66 B/48 B	
11	16:13:12	notice	accept		172.16.200.101	65.55.223.12	udp/40006	66 B/48 B	
12	16:13:12	notice	accept		172.16.200.101	157.55.235.163	udp/40014	66 B/48 B	
13	16:13:12	notice	close		172.16.210.155	208.91.113.213	HTTPS	1.32 KB/1.25 KB	
14	16:13:07	notice	accept		172.16.210.155	208.91.112.53	DNS	222 B/477 B	
15	16:13:05	notice	close		172.16.210.170	93.184.216.34	HTTP	164 B/112 B	
16	16:13:02	notice	close		172.16.210.155	208.91.113.213	HTTPS	1.32 KB/1.25 KB	
17	16:13:01	notice	accept		172.16.200.101	65.55.223.25	udp/40025	165 B/89 B	
18	16:13:00	notice	accept		172.16.200.101	157.56.52.26	udp/40023	163 B/49 B	
19	16:12:59	notice	close		172.16.210.170	93.184.216.34	HTTP	164 B/112 B	
20	16:12:59	notice	accept		172.16.210.155	208.91.112.52	DNS	0 B/0 B	

You can select a Category of logs to view by selecting from the list on the left.

The menu to the right of the Categories allows you to select a time period to view:

- Last 60 Minutes
- Last 24 Hours
- Last 7 Days
- Last 30 Days
- Specified Time Period

You can set the refresh rate of the chart by selecting the Refresh icon to the right of the time period.

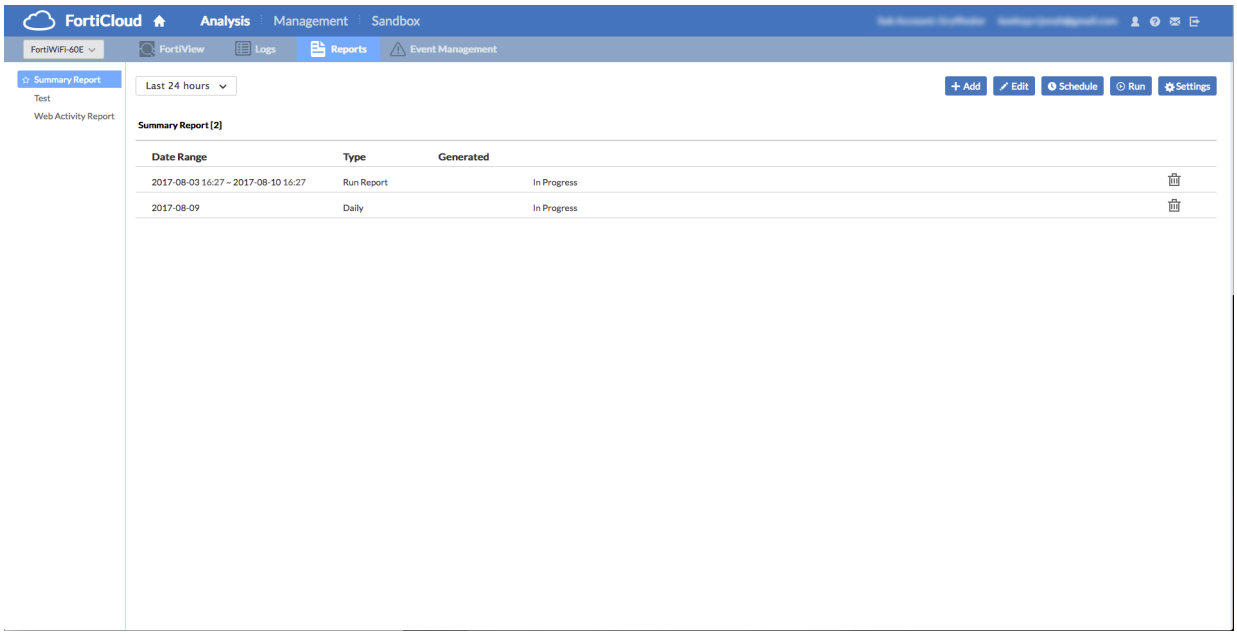
By selecting **Add Filter** in the upper right, you can filter the log list by various factors. Selecting **Column Setting** will allow you to customize the default log view.

By clicking on the "**Log Files**" text in the upper right, you can see the raw log data files, and manually download them.

The box in the lower right allows you to move through pages of log data by clicking the arrows or entering a page number.

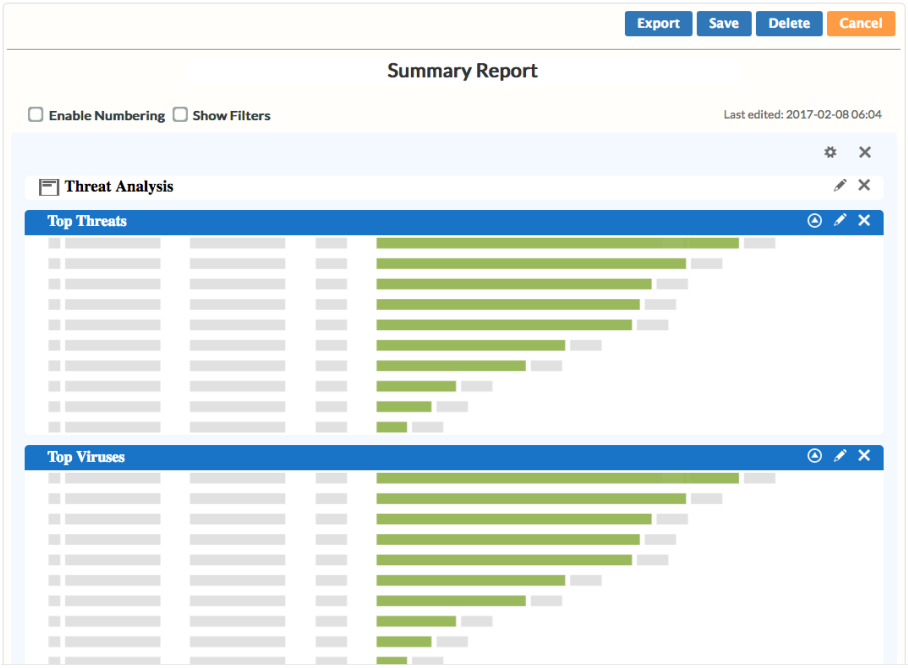
Reports

The **Reports** page generates custom reports of specific traffic data, and can email them to specified addresses.

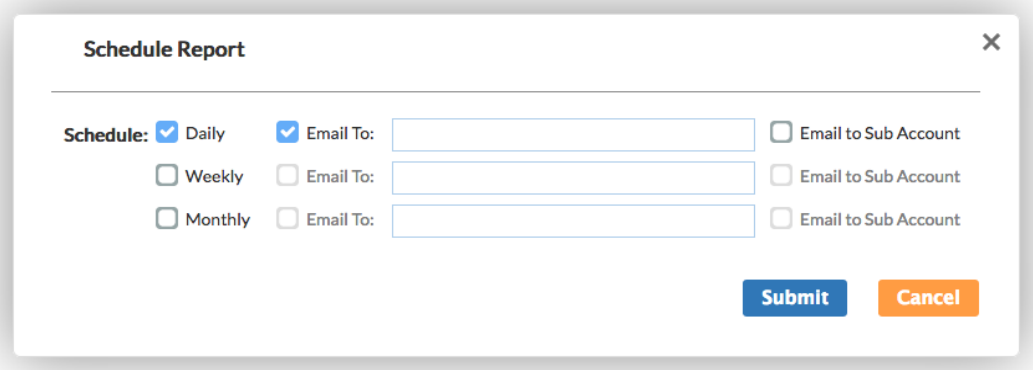


Select a report on the left to see a list of collected reports of that type: there will be a pre-configuredSummary Report and a Web Activity Report by default. Double-click on a report in the list to read it.

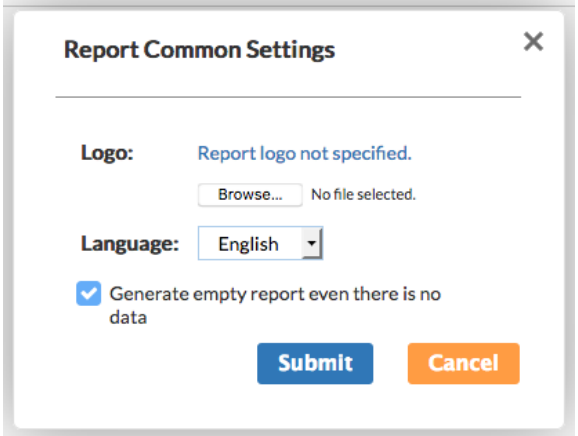
You can **Add** new reports or **Edit** existing ones in the upper right. Both of these will open an editing interface, which will allow you to edit the content of the report, adding or removing sections as you choose.



By selecting **Schedule** , you can set how often reports are run: Daily, Weekly or Monthly, and which email the reports are sent to. You can also choose to **Run** a report immediately.



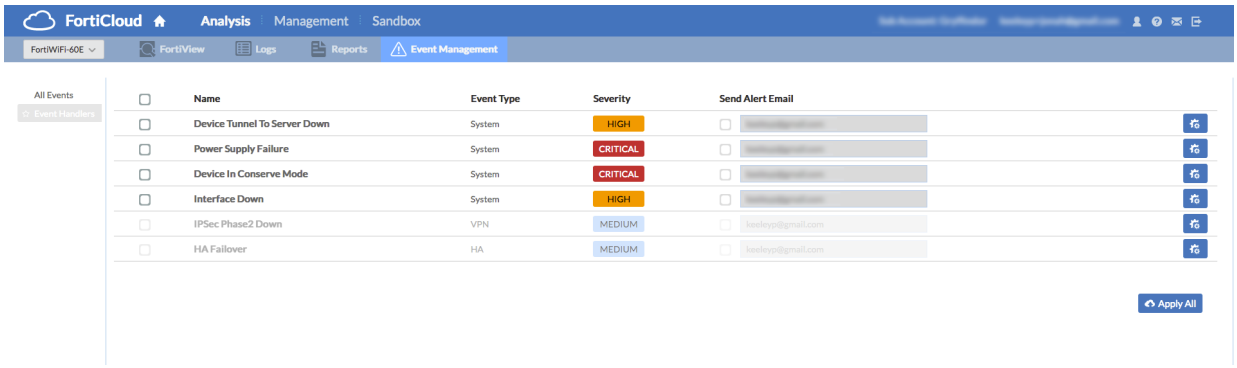
Next to the **Run** button is **Settings** where you can upload a report logo, and set the report language.



Event Management

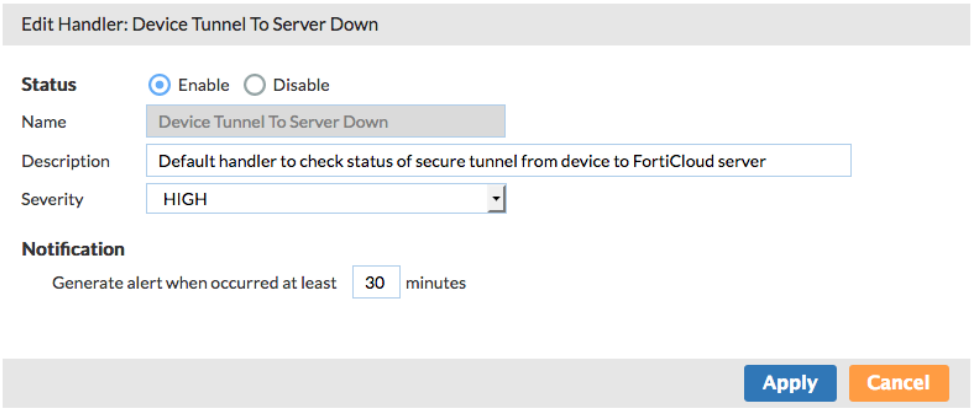
The **Event Management** page allows you to set up email alerts for specific network structure emergencies, such as FortiCloud losing connection to the device, or the device's power supply failing.

The page will default to **All Events** in the left menu, which will list all past emergency events. Select **Event Handlers** to configure the alert settings.



You can enable events to track by checking them on the left. If you'd like to recieve an alert email when they occur, check the mark under **Send Alert Email** and enter the email to send to.

Selecting the gear icon on the far right will allow you to configure each **Event Handler** directly, setting logged Severity level, and notification frequency.



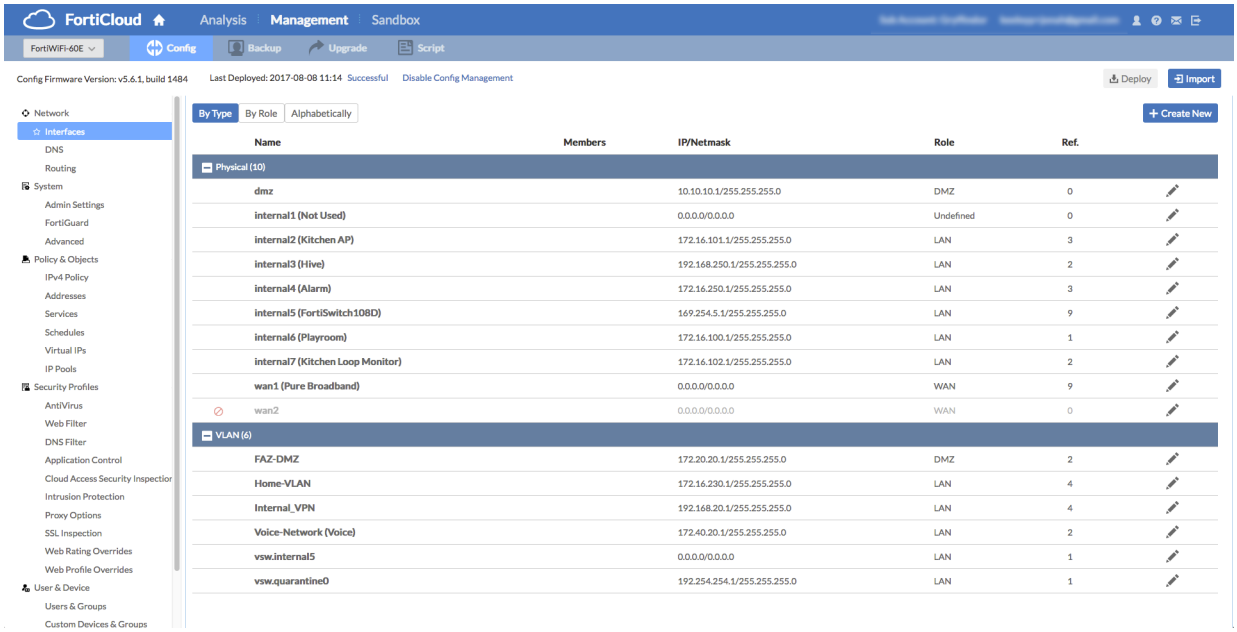
Management pages

The **Management** pages allow you to remotely manage FortiGate, FortiWiFi, and FortiAP devices that are connected to the FortiCloud service.

These pages may only appear if you have purchased a FortiCloud license, as FortiCloud Management is part of the subscription service and will not be available in the free version of FortiCloud from 3.2.1 onwards. It is available in 3.2 on a trial basis.

Config

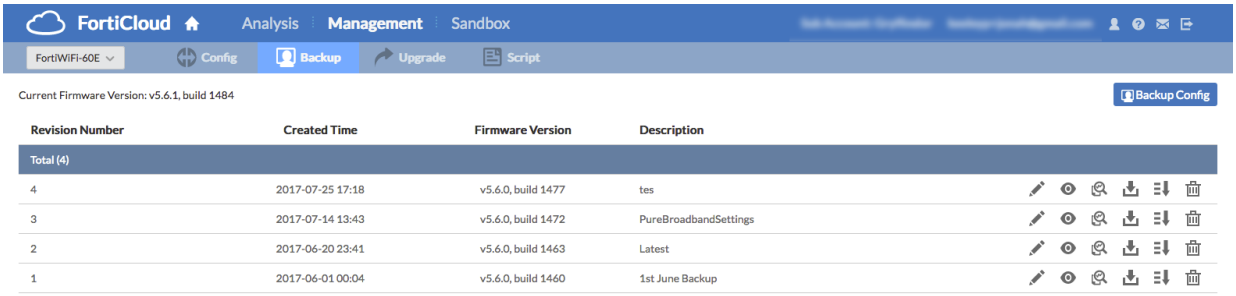
The **Config** page gives you access to a pared-down version of the remote device's management interface, allowing you to configure major features as if you were accessing the device itself.



The configuration you see in FortiCloud is not auto-refreshing; you must select **Import** from the upper right to upload the local device's config to the FortiCloud page. You can then make any changes you would like to reflect on the device, and select **Deploy** to push the configuration to the device.

Backup

The **Backup** page allows you to back up, track, and compare revisions of your remote device's configuration.

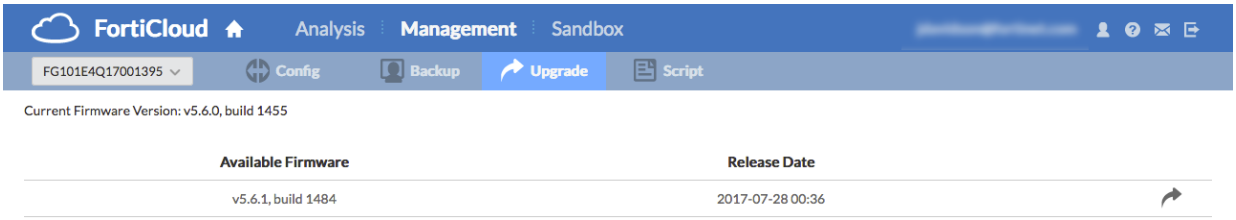


By selecting **Backup Config** in the upper right, you will save a backup to FortiCloud.

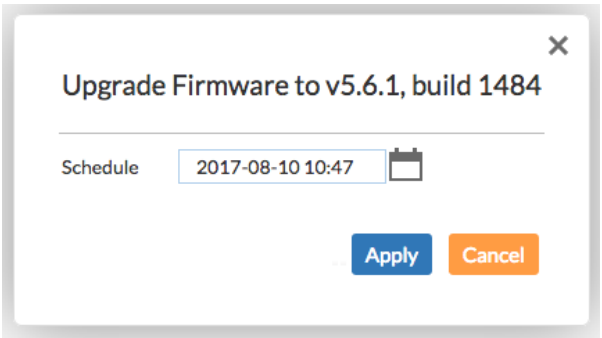
The icons on the right allow you to **Edit**, **View**, **Compare** (to other revisions), **Download**, **Restore** (to device), and **Delete** revisions.

Upgrade

The **Upgrade** page allows you to see the current firmware version installed on the device, and update to newer stable versions with one click, if they are available.

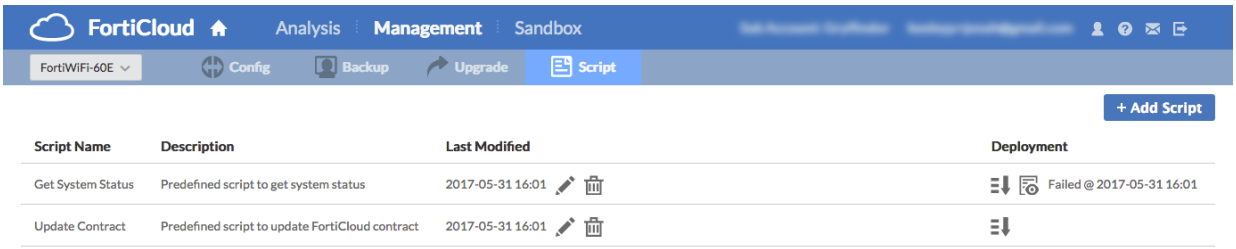


Select the **Upgrade** arrow on the right to upgrade. You can schedule a time and date to perform the remote upgrade, allowing you to schedule it during downtime to minimize disruption.

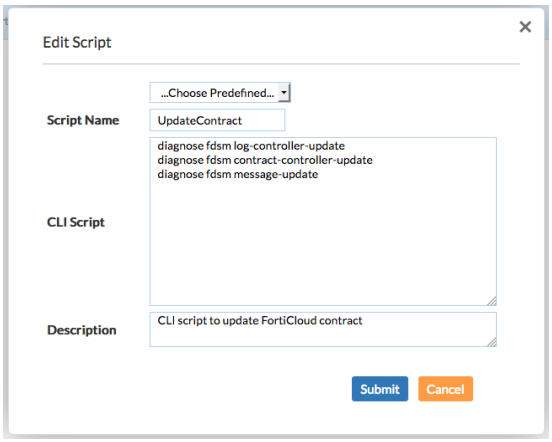


Script

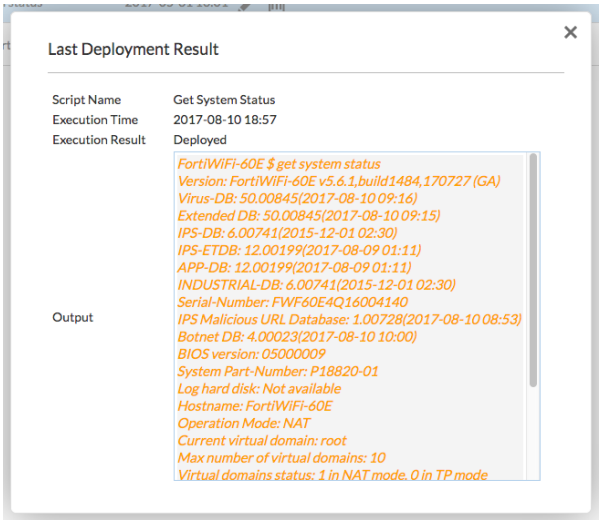
The **Script** page allows you to create and run script files on connected remote devices, allowing you to check device status or get bulk configuration information quickly.



You can click the **Add Script** button to upload a script file, or select a Predefined script, and save it. Each script is a series of CLI commands, one command per line. You can then run it on the device selected in the upper left by selecting the **Deploy** icon on the right. You can also schedule deployment for a later date or time.



The output of that script will then be recorded, and can be read by clicking the **View Result** icon on the right.

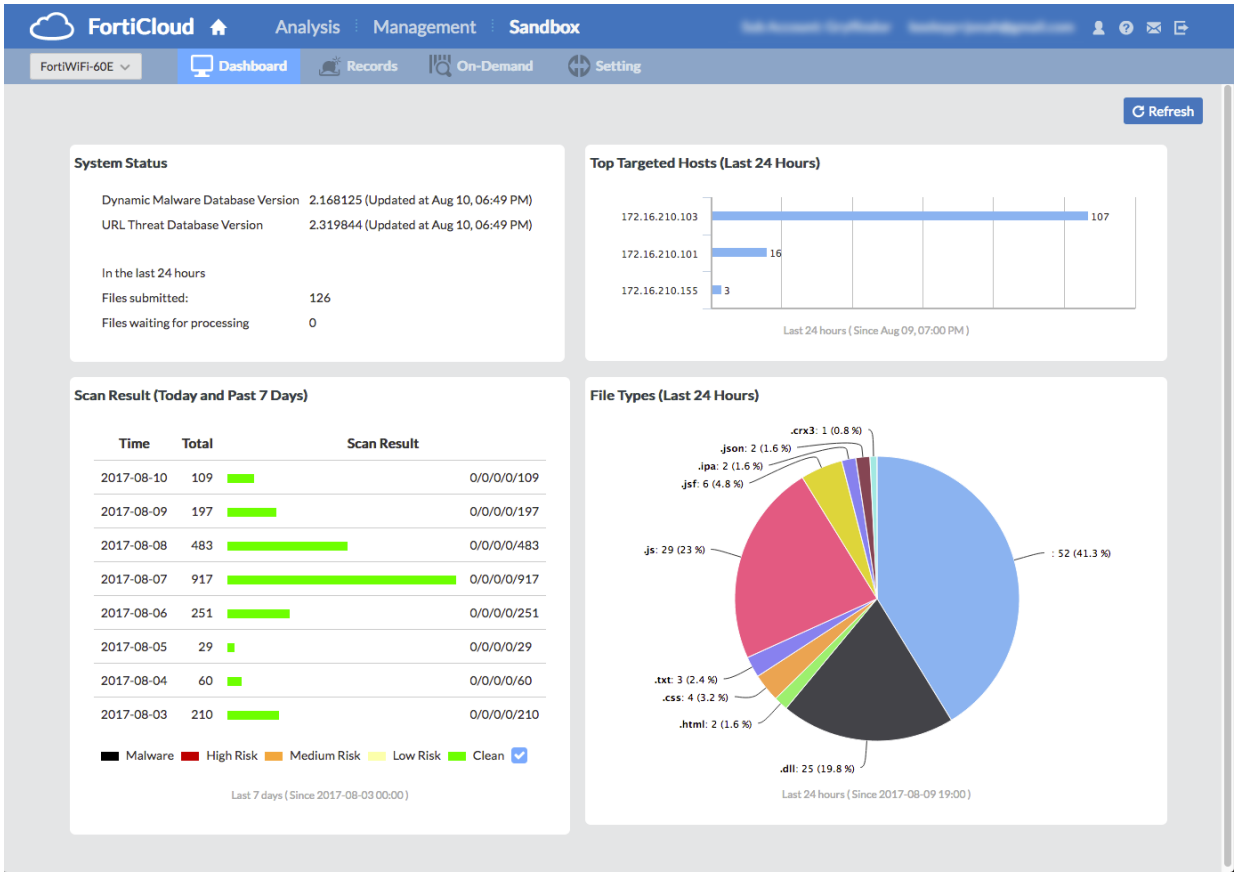


Sandbox pages

The **Sandbox** pages collect information compiled by the FortiCloud Sandbox service, which submits files to FortiGuard for threat analysis. They allow you to configure your use of the service, and view results of analyzed files.

Dashboard

The **Dashboard** page gives you an overview of the FortiCloud Sandbox results.



The Dashboard contains the following widgets:

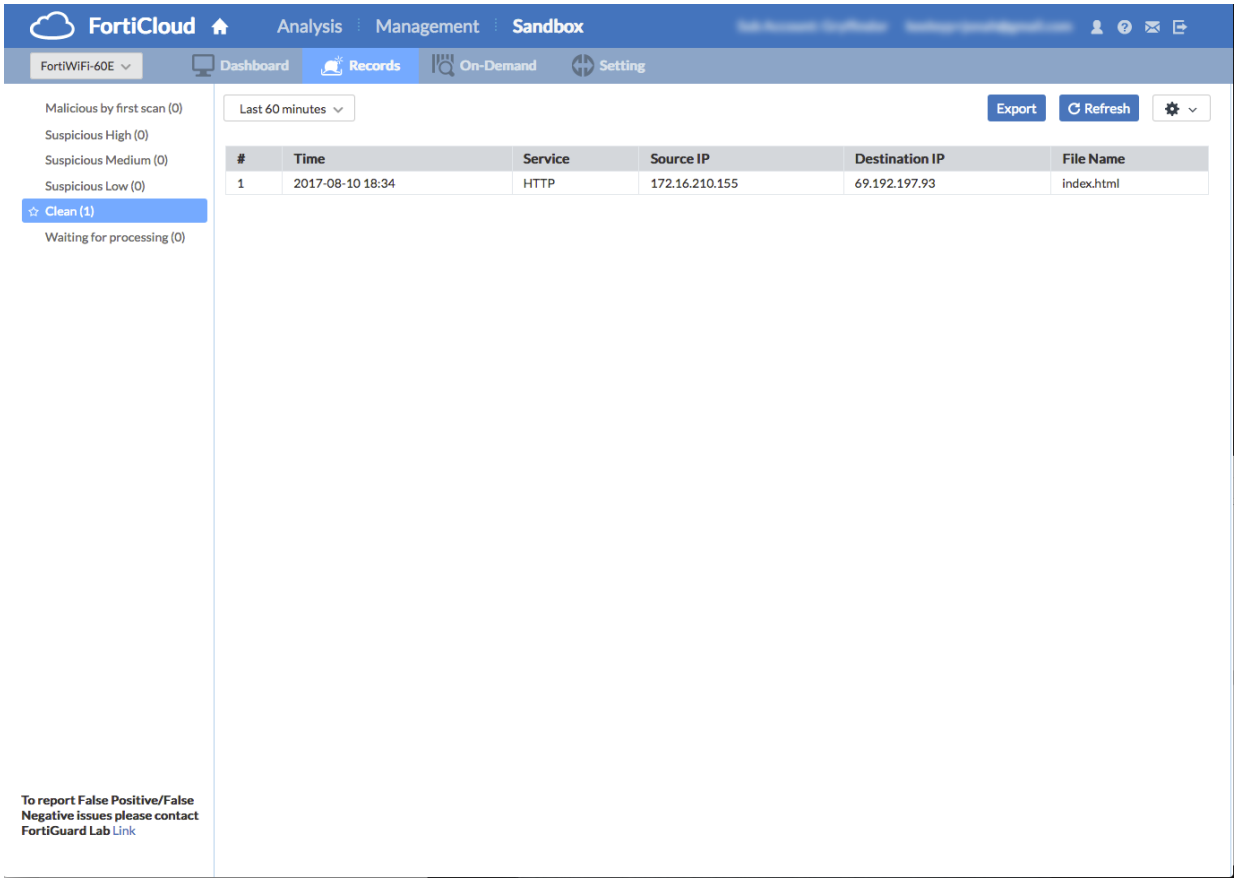
- The **System Status** widget gives you a quick view of the current state of the AntiVirus databases and load.
- The **Top Targeted Hosts** displays which hosts received the most threats.
- **Scan Result** shows the last 8 days of results and their risk levels (and you can toggle the display of Clean files in the chart by selecting the checkmark in the lower right of the widget).
- **File Types** displays the most commonly analyzed file types in the last 24 hours of scanning.

Records / On-Demand

The **Records** page displays files that have been flagged as suspicious by your connected device's AntiVirus, which have been uploaded to FortiCloud, to be analyzed by FortiGuard services.

The **On-Demand** page allows you to manually upload files to FortiGuard services to be analyzed, and displays the analysis results.

These pages may not appear if you do not have the FortiCloud Sandbox service enabled on the connected device.



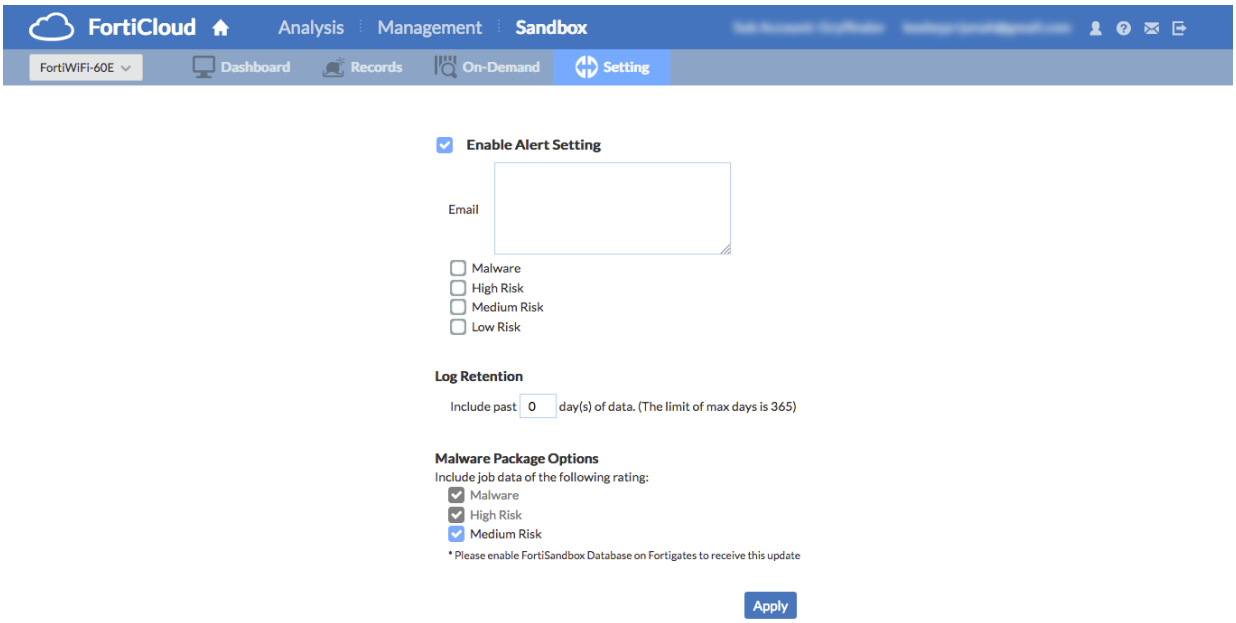
You can select an analysis level on the left, and click on the file names for more information.

The top right of the **On-Demand** page also has **Export**, which allows you to export a CSV or PDF of On-Demand results, and **Upload File**, where you can manually upload a file to be analyzed.

Maximum file size is 10Mb, and the processing time may vary based on the size of the file.

Setting

The **Setting** page allows you to configure FortiCloud Sandbox settings.



Under **Enable Alert Setting**, you can enable Alert Emails, enter multiple emails (one per line) to receive alerts, and set which level of severity will trigger alert emails to be sent.

Under **Log Retention**, you can set the number of days to retain log data.

Under **Malware Package Options**, you can select the risk level of data that will be automatically submitted to FortiGuard to further anti-threat research.

Frequently Asked Questions

General questions

What is FortiCloud?

FortiCloud is a hosted wireless and UTM infrastructure management solution and log retention service for FortiGate®, FortiWiFi® and FortiAP® devices. It gives you centralized configuration management, location-based analytics and reporting, and log retention without the need for additional hardware and software. The feature set includes:

- One-touch provisioning of large scale security and wireless networks
- Configuration and device management from a single pane of glass
- Cloud-managed FortiAPs
- Hosted log retention and cloud-based storage
- Wireless health and oversight at your fingertips
- Cloud management of wireless guest access
- Social media account login for Guest WiFi
- Rogue access point detection and analytics
- Built-in protection from APTs with FortiGuard sandboxing technology
- Location-based analytics with FortiPresence
- Instant security intelligence and analytics with FortiView
- Network health and utilization-based analytics and reporting
- Wireless configuration including security profiles per SSID for the Smart AP

What functions does FortiCloud have?

- Centralized Dashboard: system and log widgets plus real-time monitors
- FortiView Log Viewer: real-time log viewing with filters and download capability
- Drilldown Analysis: real-time location, user, and network activity analysis
- Report Generator: create custom report templates, and schedule reports in different formats to display location-based analytics or illustrate network usage patterns
- Device Management: configuration backup and history, script management, and alert profiles for real-time monitors
- AV Submission: shows the status of suspicious files undergoing cloud-based sandbox analysis
- Wireless Health Monitoring: bandwidth, usage, clients, interference, failed login and rogue APs
- Wireless Security Logs & Events: Authentication, Antivirus, IPS, Web Access, PCI compliance
- Wireless Configuration: SSIDs (including IPS, Antivirus and Web Filtering configuration), Authentication, Captive Portal, Platform Profiles, Tags and Network Settings
- Guest Management: ability to add guests and notify them if credentials via SMS or email
- Social Media Account Integration: ability for guests to connect to wireless accounts via social media

How does FortiCloud work?

One or multiple FortiGate/FortiWiFi/FortiAP units are registered with FortiCloud under a single account. This is done via the licensing widget in the device dashboard or at www.forticloud.com. The logs from each device are periodically sent to FortiCloud and stored.

Logs are sent automatically to FortiCloud for storage and processing. You configure what to log, including just Traffic and Event logs or including security logs such as Antivirus, Application Control, IPS, etc.

From the recorded logs, reports can be generated to indicate trends within network traffic, individual user activity, and security threats across different applications. Drilldown capability and real-time alerting are also available.

FortiCloud also creates copies of FortiGate/FortiWiFi/FortiAP configurations that can be used for backup and restore or to provision new devices. A VPN tunnel can be used to bring up the console of a device behind a firewall, allowing you to perform configuration or policy changes remotely.

How does FortiCloud compare with FortiPortal and FortiAnalyzer?

FortiCloud is an ideal solution for customers who do not want to implement a separate hardware solution such as the FortiAnalyzer 200D series. However, it does not have all the features of a FortiAnalyzer. A high-level comparison is shown below:

Feature	FortiCloud	FortiPortal	FortiAnalyzer
Business size	Small Branches/Large Campus/Distributed Enterprise	MSSP	Enterprise/MSSP
Summary	Fortinet-hosted cloud-based reporting, management and client sandboxing	End customer/MSSP portal, overlaid on existing local infrastructure. Hosted in the MSSP's datacenter	Premises-based log collection, reporting and alerting system
Per-Site Licensing	Licensing is based on a per-device basis.	Licensing is based on number of devices and add-ons. Devices can be FG/VDOM/wireless. No limits on scaling factors, distributed architecture.	Typical licensing for FAZ hardware. Max device limit set per model, VM and cloud-based options available.
Sandboxing	FortiSandbox Cloud included in AV bundle. FortiCloud gives visibility in cloud to uploaded files.	No support in the current release. Must use FortiSandbox.	No support. Must use FortiSandbox.
Supports external authentication for administrative access	No	Yes	Yes

Feature	FortiCloud	FortiPortal	FortiAnalyzer
Storage quota	Unlimited storage with 1 year log retention.	Based on MSSP's datacenter storage availability.	Depends on model. Up to 48 TB for the appliance, and 24 TB for the VM.
Centralized logging	Real-time for disk-less models. Batch upload for disk models.	Real-time for security and wireless, analytics and reports.	Real-time for disk-less models. Batch upload for disk models. Log aggregation and forwarding. CEF compliant logging.
Aggregated reports	No	Yes	Yes

How do I confirm which version of FortiCloud is currently in use?

Click on the FortiCloud name in the title bar, or the About link to see the build/version number.

Which languages are supported by FortiCloud?

FortiCloud currently supports two languages: English and Japanese. These can be selected via the web portal login page. Other languages may be available in other regions.

Is there any way for me to choose which Data Center my logs are stored in?

Yes. When you initially create your account in FortiCloud, it will offer you a choice of data center to use. Data and accounts cannot be transferred between data centers, so migrating will require a new account.

How can I provide feedback or request improvements to FortiCloud?

On the top right of every screen is an envelope icon, which will open a feedback submission form. Feedback is greatly appreciated, but Fortinet cannot guarantee individual responses to any requests.

Is there a European FortiCloud instance?

Yes. As of Q2 2016, the FortiCloud service has been available through our new Regional FortiCloud Datacenter, geographically aimed at our European customer base, and is completely isolated from the North American instance.

All analysis, reporting, management and storage capabilities are provided locally, with full access to our global threat intelligence databases, with the dual benefit of isolating intercontinental data and providing performance improvements and lower latency to the end device.

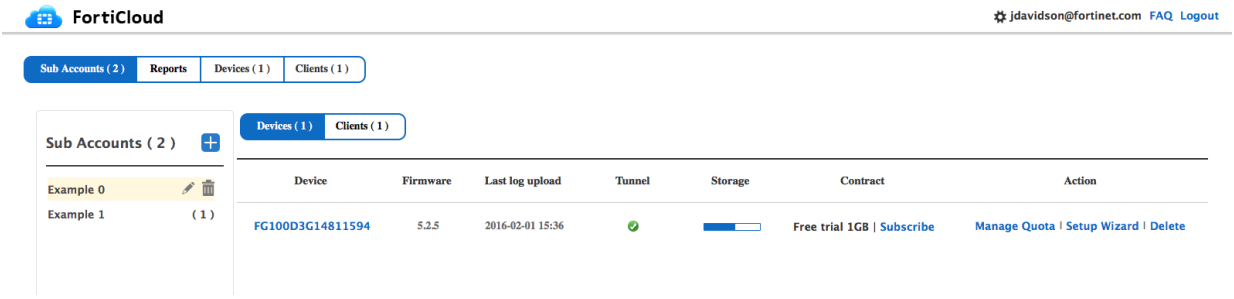
If I am an existing customer in EMEA, will my data be transferred to the new Datacenter, or will it remain in its current location?

Any existing units will remain logging to their original destinations. If you wish to change this, please contact our Customer Services. No existing logs will be moved as part of this process.

Is there an account designed for MSSP-scale operations?

FortiCloud has a premium account type, designed for Managed Security Service Providers: a Multi-Tenancy Account.

A Multi-Tenancy Account is a one-year service for an administrator to create and manage multiple sub-accounts. It also allows devices to be moved between these accounts. Each of the sub accounts can be allocated administrators, with full or read-only access, allowing you more control over the provision of a managed service.



To activate a Multi-Tenancy Account, please request a quote for the following SKU:

"**FCLE-10-FCLD0-161-02-DD**"

through your Fortinet Partner or Reseller.

What are the new features in Version 3.3.0?

Zero-Touch Deployment for Multi-Tenancy accounts

Zero-Touch Deployment is a new deployment concept, first available in 3.3.0. New FortiGate devices are added to your existing FortiCloud account upon purchase, and a pre-selected and customizable configuration template is automatically installed as soon as the device is deployed. This allows you to airdrop devices into new remote offices or branch locations, and ensure that they are already pre-secured and ready to use, integrated into your FortiCloud monitoring. It also offers convenient setup for bulk purchase of devices, with devices automatically syncing and configuring themselves upon arrival.

Also included alongside Zero-Touch Deployment are a number of features which make it possible, which can be individually configured and used for remote device management:

- Creation and deployment of pre-defined configuration templates, to one or multiple devices
- Easier deployment and control of FortiOS version updates for connected devices
- The ability to select which specific FortiCloud accounts/sub-accounts you want to deploy to
- Config file visibility and diff comparison when pushing config changes to remote devices, allowing for easier administration and troubleshooting.
- Password verification is now required for devices that are not at factory default, for a secured management layer

FortiGate management

Multiple updates have been made to the FortiGate management interface, improving and adding new features:

- VPN configuration through FortiGates (with and without the VPN Wizard), and VPN traffic appearing in FortiCloud Reports and FortiView
- Added new pages: DNS, Multicast Routing, Traffic Shaping
- Improved usability of pages: Policies, Security Profiles, User & Device

Improved device and service integrations

FortiSwitch

You can now manage FortiSwitch devices that are networked with connected FortiGates, with full management of interfaces and VLANs, FortiLink awareness, and integrated device and PoE information.

FortiView

The FortiView interface in FortiCloud has been improved and expanded to include the new FortiOS integrations.

Also, FortiCloud is once again available as a source for FortiView in the FortiOS management interface.

FortiExplorer

The FortiExplorer Application has been integrated into FortiCloud.

Extended FortiAP management features

3.3.0 has introduced a number of new FortiAP management features, with a focus on architecture improvements:

- Extended API to include FortiAP Guest and Rogue AP feature sets
- Added wireless mesh configuration
- Added ability to isolate Guest accounts without VLANs
- Integrated multiple PSK support
- Added ability to choose firmware upgrade time

Single-use FortiCloud keys

All FortiCloud registration keys are now single-use, and cannot be used again without contacting Fortinet Support, to protect management accounts from compromise.

What was added in previous versions?

3.2.1

FortiGate management

A FortiCloud-enabled FortiGate can offload FortiView processing to the remote server, allowing for improved FortiView efficiency.

Multi-Tenancy improvements

The Multi-Tenancy dashboard provides better management of multiple devices with the addition of filtering, sorting, and group management. These new capabilities can help you perform bulk actions. For example, you can run bulk scripts on all grouped devices, to initiate mass upgrades or resolve new CLI changes. For

compliance or standardization purposes, you can create Configuration Templates, and then apply them to grouped devices.

AP Network improvements

Change History logging is available to document AP Config changes. MAC Access Control is now available in AP Configuration, with the ability to set individual MAC Access rules per AP, and the function to import lists of MAC Addresses. Configure Fail Through mode to enable Captive Portal networks to authenticate without MAC Address matching.

Captive Portal also allows for Self-Registered Guests. You can customize the registration page, account expiration, and other settings in the FortiCloud dashboard. Self-Registered users have their own section in the AP Network user list.

3.2

The major feature in 3.2 is FortiGate Configuration Management, which allows for synching of connected FortiGate devices, uploading and downloading their config files and making in-FortiCloud changes that can then be reflected in the devices.

FortiGate Configuration Management is included as part of the FortiCloud Subscription service. In 3.2.0, it is available to all FortiCloud users as a trial, but as of 3.2.1 it will require a 1 Year Management, Log Retention and Analysis Contract. At that point, you will be able to view device configurations without a contract, but will no longer be able to edit them.

This feature advances FortiCloud as a universal cloud management platform, and many other small features have been added in 3.2 to support this concept:

- more visibility and detail from FortiView
- simpler Log viewing with a log data sidebar
- FortiGate Event Management (with alert emails for events such as Device Tunnel Down and Power Supply Failure)
- Config Deployment Scheduling, allowing you to schedule remote config uploading, firmware upgrades, and scripts
- On-Demand submission of files to FortiCloud Sandbox for analysis

AP Network and MSSP features have been updated in 3.2 as well, with remote FortiPresence configuration, QoS Profiles, increased IPS capabilities, preliminary support for FAP-U models, AP Network alert emails, and a new REST API for querying AP Network information.

The API is currently only available on a limited basis. Contact Fortinet Support if you require access.

3.1

Two-Factor Authentication has been added to the management interface. FortiGate management remains as a public beta service in 3.1, but has been expanded to allow importing of the current configuration from a deployed FortiGate. Sandbox functionality has also been improved, showing the number of files waiting for processing.

A new Enterprise-level license is now available as a paid upgrade for connected APs, covering a number of advanced RF settings, and blocking of intra-SSID traffic. This license includes support for the FAP-S series APs, with included FortiGuard subscription and Bonjour relaying support.

3.0

Location-based analytics with FortiPresence have been added. To support FortiPresence features, social media logins for Guest WiFi Accounts have been integrated into FortiCloud. Also new in 3.0 was enhanced FortiOS

management, Fast Roaming between AP units, and enhanced AP configuration in NAT Mode.

2.5

Multi-tenancy was added; and a series of wireless-related features such as guest management, external captive portals, security per SSID (for the Smart AP), AP location floor plan and AP radio adjustment. Also added were PCI compliance reports and integration with Advanced Threat Protection.

Licensing and registration

Is there an easy way to test drive FortiCloud?

Yes, you can test drive FortiCloud by visiting the FortiCloud portal, and selecting the Live Demo link at the bottom of the FortiCloud login screen. This will show a FortiCloud account with populated devices and logs to simulate a live environment.

What is the price of FortiCloud?

A no-charge service option is available with unlimited storage is available for one week.

Effective in FortiCloud 3.0, we are replacing the 200Gb-per-device service with a annual-subscription-based service, with one, two, or three-year service terms.The new service provides 1 year of history, regardless of size.

FortiCloud will be available for all FortiGate devices up to the FG3200D.

To activate FortiCloud after the free trial ends, you will need to acquire a subscription license based on the following SKUs, available with 1, 2, and 3-year service terms:

Description	SKU
FortiCloud Analysis and 1-Year Log Retention	
FortiGate (Up to 2U) & FortiWiFi	FC-10-00XXX-131-02-DD
FortiCloud Enterprise AP Licenses	
FAP/FAP-U/FAP-C	FC-10-90AP1-170-02-DD
FAP-S	FC-10-90APS-170-02-12
FortiCloud IOC (Indicator of Compromise)	
FortiGate FGT20-90 models	FC-10-90803-142-02-12
FortiGate FGT100-300 models	FC-10-90804-142-02-12
Other Services	

Description	SKU
FortiCloud - Multi-Tenancy	FCLE-10-FCLD0-161-02-12
FortiDeploy Access	FDP-SINGLE-USE

Activation on device requires FortiOS 5.4.2 or newer. The Indicator of Compromise (IOC) Service requires an existing FortiCloud subscription.

For pricing information, please contact your Fortinet partner or reseller.

Do I need a support contract to enable the service?

No, but you do need to register each FortiGate/FortiWiFi/FortiAP on the Service and Support Portal at https://support.fortinet.com. It's very important to register each device in your network, or the service (free or subscribed) cannot be enabled.

How do I subscribe to a FortiGate Analysis and Log Retention contract?

To upgrade to a subscription, you need to:

1. Obtain a license (Contract Number) from your Fortinet reseller.
2. Click on the Upgrade icon in the FortiGate/FortiWiFi dashboard licensing widget.
3. Follow the instructions presented. If you are running FortiOS 5.0 and higher, you have the option of receiving a scratch-off card/certificate from your Fortinet reseller.
4. Scratch the card to reveal the hidden activation code. Enter this directly into the FortiGate console in the Licensing widget.
5. Wait about 30 minutes for the backend systems to process the subscription.
6. Check your FortiGate/FortiWiFi Dashboard, and the subscription will have changed from Free to Subscribed.

What features do I get access to for subscribing?

Yes. When you upgrade to a subscription, you will no longer have a daily limit on uploads and will be able to create, schedule, and customize reports. You will also be able to subscribe to more advanced features, like the FortiCloud IOC (Indicator of Compromise) Service, FortiPresence Analytics, and FortiOS Management.

You also gain the ability to analyze more files per day with FortiCloud Sandboxing (the free version limits you to 100 files per day.) The actual daily limit of files is based on the model of FortiGate deployed.

How do I subscribe to the Enterprise License?

1. Place an order, and receive a Support Contract from your selected partner.
2. Per the Service Entitlement Summary on the contract, apply the Contract Registration Code on support.fortinet.com.
3. Select the applicable FortiAP (S) serial number.
4. Complete the registration process.
5. Product Entitlements will now display Support Coverage for 'FortiCloud FAP Management Service' with a 1-year subscription.

What features do I get access to for subscribing to the Enterprise License?

FortiAP-C benefits from 8x5 support and 1-year log retention.

FortiAP and FortiAP-U also gain advanced wireless features which grant control over transmitted data rates.

FortiAP-S benefits from the additional capability of Bonjour relaying, a subscription to FortiGuard services, and intra-SSID isolation of specific clients.

More subscriber-only features will be added in future releases of FortiCloud.

What happens if I lose my password?

You can reset your password on the FortiCloud portal at https://www.forticloud.com.

Can I use Two-Factor Authentication for FortiCloud?

Yes. As of 3.1, Two-Factor Authentication is offered as part of the base free service, using the FortiToken app available on mobile devices. To enable two-factor authentication, ensure your entered email address is correct, as you will be sent an email withe setup instructions. Then enable '2-Factor' in the 'My Account' section.

How do you configure service once it is activated?

The configuration of the service is done via the web portal at https://www.forticloud.com. The logs will automatically start appearing in the logs and archives section.

Select the gear icon on any page to edit that page's settings.

Select the gear icon next to the administrator email in the top right to edit user settings.

For how long are logs retained?

FortiCloud will automatically delete logs older than the length of the support contract to make space for new log data. Email and pop-up reminders will be sent periodically (30 days, 14 days, 7 days, and 24 hours) before logs are deleted and before the contract term comes to an end.

When a device subscription lapses, what happens to the year's worth of logs?

Any logs that are associated with the licensed device older than 1 year will be automatically purged. For the free service, logs older than 7 days will be purged.

There is no grace period, so please ensure you are properly renewed so that your logs are retained.

What if I want to unsubscribe from the service and stop uploading logs?

You can disconnect your account from the dashboard in your FortiGate/FortiWiFi. In the Licensing and Information widget in the FortiGate interface, click on the Log-out button. This will detach the FortiGate/FortiWiFi from the account and stop the logs from uploading.

Technical questions

What security and redundancy has been built into the service?

Logs are transferred between devices and the FortiCloud storage are transmitted via an encrypted link. All system elements are duplicated for redundancy.

How do I verify my network is PCI compliant?

FortiCloud makes it easy to deploy, monitor and verify PCI compliance. FortiCloud's security feature set addresses PCI Data Security Standards 3.0, helping customers to build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong control measures, and monitor network security.

Does my FortiGate unit require a hard drive to use FortiCloud?

The FortiGate does not require a hard drive if logs are being uploaded to FortiCloud in real-time, which can be enabled in the Log Setting page in the FortiGate interface. FortiCloud is a convenient alternative to a hard drive for devices too small to contain one, such as FortiWiFi units.

Does FortiCloud support devices from other vendors?

FortiCloud only supports FortiGate, FortiWiFi and FortiAP products. It does not currently support other company's products for log retention.

Which FortiGate and FortiWiFi models does FortiCloud support?

FortiGate

All 2U (3200D) and smaller FortiGates are supported by the FortiCloud environment.

FortiWiFi

All FortiWiFi models 20 to 90 support FortiCloud natively through the dashboard Licensing widget.

FortiAP

All FortiAP, FortiAP-S, and FortiAP-C models are supported by FortiCloud. FortiAP-U will be supported by Q3 2017.

Which versions of FortiOS does FortiCloud support?

FortiCloud is available for all devices at FortiOS version 4.3 or later, but for full feature support, the most current available version should be deployed. Devices running FortiOS version 4.2 or earlier may not be able to access FortiCloud. Consult your device's documentation for more information.

What port numbers are used by FortiGate devices connecting to FortiCloud?

Please note that these should be required by outbound traffic only. On request, we can supply the destination IP addresses to add to an outbound policy, if required.

Purpose	Protocol/Port
Syslog, Registration, Quarantine, Log & Report	TCP/443
OFTP	TCP/514
Management	TCP/541
Contract Validation	TCP/10151

When are scheduled reports sent to administrators?

Scheduled reports are sent to administrator email addresses between 2 AM and 6 AM if automatic report delivery (Daily/Weekly/Monthly) is enabled.

Why can I not see any management functions?

You must first enable the management tunnel on the FortiGate/FortiWiFi device. On the device, use the following commands in the CLI:

```
config system central-management
   set mode backup
      set type fortiguard
   end
end
```

Can I set up high availability (HA) logging with FortiCloud?

FortiCloud accepts inbound logs from each device independently, and has no means of detecting that connected devices are in an HA cluster. Though multiple HA clustered devices will theoretically send identical logs to FortiCloud, if one device stops logging or is unable to reach FortiCloud, the other devices will not send logs on its behalf.

Do I need to purchase a subscription for each FortiGate in an HA pair?

Yes. FortiCloud handles each device separately, regardless of configuration.

FortiCloud Sandbox

How does Cloud Sandboxing and AV Submission work?

In a proxy-based antivirus profile on a FortiGate, the administrator selects Inspect Suspicious Files with FortiGuard Analytics to enable a FortiGate unit to upload suspicious files to FortiGuard for analysis. Once uploaded, the file will be executed and the resulting behavior analyzed for risk. If the file exhibits risky behavior or is found to contain a virus, a new virus signature is created and added to the FortiGuard antivirus signature database. The next time the FortiGate unit updates its antivirus database it will have the new signature.

FortiGuard Labs considers a file suspicious if it exhibits some unusual behavior, yet does not contain a known virus (the behaviors that FortiCloud Analytics considers suspicious will change depending on the current threat climate and other factors).

The FortiCloud console enables administrators to view the status of any suspicious files uploaded: Pending, Clean, Malware, or Unknown. The console also provides data on time, user, and location of the infected file for forensic analysis.

Why can I not see a function or tab for AV Submission/Sandboxing?

You must first enable Cloud Sandboxing on the FortiGate device, and then submit a suspicious file to cause the tab to appear.

What is the turnaround time on Cloud Sandboxing and AV Submission?

It can be anywhere from 10 minutes (for automated sandbox detection) to up to 10 hours (if FortiGuard Labs is involved).

Is there a service description for FortiCloud Sandbox?

Yes, a full current service description is available online here:

http://docs.fortinet.com/uploaded/files/3429/FortiSandbox-Cloud-Service-Description.pdf

AP Network

What is the FortiCloud AP Network feature?

This feature allows administrators to remotely configure APs, modify wireless management settings and visualize wireless-related events. Examples of configuration changes include AP name and SSID configuration, power settings and rogue AP detection. Wireless management settings include RADIUS details, standard users/groups/guests and SSIDs/security. There are a robust set of visualizations including real-time and historical charting of traffic usage, AP client counts and client usage. Think of it as a comprehensive way to manage your wireless infrastructure via the cloud.

How can I register a FortiAP to my FortiCloud account?

Supported FortiAP models include a sticker with a unique FortiCloud key affixed. This key must be entered into the FortiCloud interface to register the FortiAP to your FortiCloud account.

What is the recommended FortiAP version to use with FortiCloud 3.2?

We recommend FortiAP version 5.6 or later for use with FortiCloud 3.2. It is always our recommendation that you run the latest GA firmware on your FortiAPs.

What port numbers are used by FortiAPs connecting to FortiCloud?

Please note that these should be required by OUTBOUND traffic only. On request, we can supply the destination IP addresses to add to an outbound policy, if required.

Device	Purpose	Protocol/Port
FortiAP, FortiAP-S, FortiAP-C	Initial Discovery	TCP/443
FortiAP, FortiAP-S, FortiAP-C	CAPWAP Tunnel, Event Logs	UDP/5246, UDP/5247
FortiAP, FortiAP-S, FortiAP-C	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
FortiAP-S	FortiGuard	UDP/53, UDP/8888

What happens if my AP loses connection with FortiCloud?

If your AP loses connection to FortiCloud, or in the unlikely event that the FortiCloud service is unavailable, then all functions which are not hosted in FortiCloud will continue to work without interruption. The configuration is held locally on the AP, and will continue to function.

Only SSID's with authentication in FortiCloud will be disrupted: FortiCloud-hosted Captive Web Portals, and FortiCloud User Groups. Open, WPA2 PSK, and WPA2 802.1X RADIUS SSID's that are not using FortiCloud-hosted authentication (such as ones using local RADIUS server or Local Captive Portal) will continue to work uninterrupted.

I have an older FortiAP that doesn't include a FortiCloud key. Is there some way I can add my device to a FortiCloud AP Network?

Older FortiAPs that have shipped without a FortiCloud key can be added to FortiCloud. Open the FortiAP management interface, and in **WTP-Configuration** select **FortiCloud**. Enter your FortiCloud credentials, and select **Apply**. Login to FortiCloud and select **Inventory > Unused APs** to see the list of FortiAPs. Select **Deploy to AP Network > Existing AP Network**.

What FortiAP models are supported by FortiCloud AP Networks?

The AP Network functionality within FortiCloud is supported by all FortiAP models.

Does the FortiCloud AP Network feature support FortiWiFi?

FortiWiFi models are not currently supported for wireless configuration.

Is there a minimum firmware version that I need to run on a FortiAP for the FortiCloud AP Network feature to work?

The FortiAP must be running FortiAP OS 5.2 at a minimum. It is recommended to run the latest software build on the FortiAP to guarantee FortiCloud functionality.

Does my internal wireless/networking traffic get sent to FortiCloud?

No. Fortinet uses an out of band management architecture, meaning that only management data flows through the FortiCloud infrastructure. No user traffic passes through Fortinet's datacenters, and your data stays on your network.

Do I need to use a FortiGate in conjunction with a FortiCloud AP Network?

No. We recommend you register your FortiAP to be directly managed by FortiCloud. You do not need to use a FortiGate unit as a proxy to manage FortiAPs from FortiCloud.

Is there different pricing/licensing for AP Network functionality?

There are no additional fees or licensing required to manage FortiAPs from FortiCloud.

Can FortiAP devices be managed by FortiCloud and work with FortiPresence?

Yes, FortiPresence is supported by FortiAPs and managed by FortiCloud in version 3.1.

For location analytics, the APs will use a Push API to talk to the FortiPresence cloud. You can configure this under **AP Network > Configuration > Miscellaneous**.

Is there a maximum number of FortiAPs that can be managed via FortiCloud?

There is no licensing limit for the number of FortiAPs that can be managed with FortiCloud.

How does roaming work for a FortiCloud managed AP?

Starting with FortiAP 5.4 and FortiCloud 3.0, APs which are in the same management subnet will talk to each other using encrypted communications and share station and authentication information. This means that when a client connected via Captive Web Portal, 802.1X or PSK moves from one access point to another, there is no re-authentication required and a session transition should happen once the client decides to roam.

What is the admin password for my AP?

When you add an AP Network, you are asked to define a password for it. This password is used as the admin password for all APs inside that AP Network. The password can be changed inside the AP Network under **Configuration > Miscellaneous**.

What is Social Media Captive Web Portal?

Social Media Captive Web Portal is the functionality that creates a Captive Web portal where a user's social media login is used as authentication. This is hosted in FortiCloud, and currently supports Facebook, Google+, LinkedIn and Twitter accounts. The Captive Web Portal can be customized with different colors and logos.

We recommend a Terms of Use be added to the Captive Web Portal, matching with the legal requirements of your jurisdiction. Please see the disclaimer on the configuration page for more details.

What is Self-Registered Guest Captive Portal?

Self-Registered Guest Captive Portal is the functionality that creates a Captive Web portal that requires a user to create an account, by specifying some information you choose. You can choose what form the username takes, and the Captive Web Portal can be customized with different colors and logos.

We recommend a Terms of Use be added to the Captive Web Portal, matching with the legal requirements of your jurisdiction. Please see the disclaimer on the configuration page for more details.

What is the NAT IP Subnet of my AP SSID Configuration?

If you want each AP to provide its own AP NAT boundary rather than bridge users directly onto the local network, you can now assign the Subnet for the APs to use in the SSID configuration.

Note: A known limitation is that the subnet will be assigned only on the 2.4Ghz radio. The 5Ghz radio will use a subnet 17 octets higher. For example, if the 2.4Ghz radio is set to use 10.10.10.1/24, the 5Ghz radio will use 10.10.17.1/24. This limitation will be addressed in a future software release.

What is Floorplan in Maps?

In FortiCloud 3.0, you can now add a Floorplan, and zoom into it to place your APs and see their statistics and RF information. Previously, you could use Google Maps integration to see a floorplan overlaid over a building, but now full zoom and positioning controlls have been added.

What are Folders?

Folders are a simple way to group AP's together for management purposes, and can be used to organize APs into groups, sites or any other organization you see fit. You can create subfolders and also assign new addresses and locations to APs.

How do Dynamic VLANs work?

RADIUS servers can be configured to pass class attributes back in response to a successful authentication. One of these attributes is the VLAN to which the client should be assigned. With an Enterprise license and this feature enabled, it is possible to place different types of users connected to the same SSID into different VLANs, based on their user credentials.

What is Bonjour Relay?

Bonjour is a protocol where (typically Apple) devices broadcast their services. For example, an Apple TV sends a Bonjour broadcast, so that an iPad knows it is there and can connect to it.

The issue is that these broadcasts are layer 2 – so if the iPad and the Apple TV are on different VLANs, then they will not be able to talk. Bonjour Relay is a simple mechanism to fix this. The FAP-S series of APs can be set to operate with a service network (where the Apple TV is), and a client network (where the iPad is), allowing the FAP-S to re-transmit the Bonjour requests from the service network onto the client network, allowing the iPad to learn where the Apple TV is and create a session.

To set it up, enter one or more services as Service VLAN and Client VLAN, along with a definition of the service, e.g. you may choose to only send the information about the Apple TV to a meeting room, and not the printer in reception. Once these services have been defined, simply select the AP that will perform the Bonjour Relay function.

What is Blocking of Intra-SSID Traffic?

This feature blocks all traffic from one client to another on the same SSID. This helps to avoid a common issue of clients sending data between themselves on the same SSID, without traversing and being protected by the firewall.

Why do I need to change my Radio Rates in the Enterprise Management section?

Wireless operates at many different data rates based on the quality of the radio signal. For example, an 802.11n 2.4GHz client is capable of running at 450 Mbs on a 3x3 AP, but it is equally capable of running at 1 Mbps.

Inconsistent radio rates can lead to clients remaining connected to an AP long after they should have reconnected to a better AP. A client running at 1 Mbps has great range, but its slow throughput will have a degrading effect on the network performance as a whole. The new data rate control feature in 3.1 allows you to restrict which data rates are allowed, to ensure clients that are too far away are not slowing down the overall system.

Indicator of Compromise (IOC) Service

What is the FortiCloud Indicator of Compromise Service?

FortiCloud Indicator of Compromise (IOC) Service is a new service that alerts administrators about newly-found infections and threats to devices in their network. By analyzing UTM logging and activity, the service can provide a comprehensive overview of threats to the network.

What kind of threats can the IOC Service detect?

IOC can detect three types of threats, based on our evolving FortiGuard database:

- Malware — Malicious programs residing on infected endpoints.
- PUP — Potentially unwanted programs, such as Spyware, Adware, and toolbars.
- Unknown — Threats detected by signature but not associated with any known malware.

How do I get access to the IOC Service?

The free version of IOC is currently available on all accounts in the North america data center.

Non-Multi-Tenancy Account

In the FortiGate list, look for red 'Threats/Suspicious' text underneath the System Status, which will only appear if the FortiGate has detected any threats. Click on the text to open the IOC interface.

Multi-Tenancy Account

In the FortiGate list, look to the far right. A 'bomb' icon will be visible next to the other configuration icons, if your FortiGate has detected any threats. Select the bomb icon to open the IOC interface.

Does the IOC Service require a subscription?

The basic form of the IOC is free, which will alert you to threats and automatically prepare a comprehensive threat report. Threats listed will only provide partial IPs of infected devices: server and subnet.

You can purchase a subscription for the complete IOC by opening the How to Buy page in the FortiCloud IOC site, and completing the purchase process.

A subscription grants you access to IP Whitelisting, which allows you to narrow your malware search by excluding safe IPs and domains, and Alert Emails, which notify you directly of detected network threats. It will also allow you to view the full IPs of infected devices, allowing you to better control their access to your network.

How do I register my subscription code once I've purchased one?

You will receive your subscription code by email. Visit the Fortinet Support portal at http://support.fortinet.com, and log into your customer account. On the Asset page, register the subscription code as if it were a product serial number, and then enter the serial number of the FortiCloud-connected device that you want the service to monitor.

FortiDeploy

What is FortiDeploy?

FortiDeploy is a product built into FortiCloud as a feature, for one-touch provisioning when devices are deployed, locally or remotely. FortiDeploy provides deployment for FortiAPs into a Cloud AP Network, and automatic connection of FortiGates to be managed by FortiCloud or a FortiManager unit.

What features does FortiDeploy provide?

- One touch deployment for FortiAPs into a Cloud AP Network
- One touch deployment for FortiGates to be FortiCloud managed or mananged by a FortiManager IP

How does FortiDeploy work?

When you visit forticloud.com and enter the Bulk FortiCloud Key, you will see a list of serial numbers from the order that contained the FortiDeploy SKU. Once you confirm that the devices are connected, you can perform some basic configuration on the devices remotely, such as sending a FortiManager IP to all remote FortiGate devices, so they can be managed remotely.

How do I purchase FortiDeploy?

At time of purchase, order a FortiDeploy SKU in addition to your other purchases, and enter it in FortiCloud. Once the FortiGate's serial number is associated with your customer account, you have the option to deploy the devices in either FortiCloud or FortiManager. FortiDeploy can also push an IP to each FortiManager. Support starts the moment you send an email to cs@fortinet.com.

What is the price of FortiDeploy?

FortiDeploy must be purchased on every PO using FDP-SINGLE-USE SKU. The nominal fee is $100/PO.

What happens if you forget to order FortiDeploy on the PO?

If you forget to order FortiDeploy on the PO, please send an email to the Fortinet Customer Service and Support Team: cs@fortinet.com, and they can manually register your serial numbers and generate a Bulk FortiCloud Key.

Will my FortiGuard and FortiCare services start automatically?

No. FortiGuard and FortiCare services will start only after you register your serial numbers. Bulk registration of FortiGuard and FortiCare is available, but you will need to send a direct request after registration to cs@fortinet.com.

What are the devices supported by FortiDeploy?

- While FortiCloud supports all FortiGates up to the 3240C, FortiDeploy is only available up to the 200E, as we recommend that larger deployments be handled by trained personnel.
- All FortiWiFi devices
- All FortiAP devices

Which versions of FortiOS does FortiDeploy support?

FortiDeploy is available for FortiGate/FortiWiFi devices at FortiOS version 5.2.2 or later, and FortiAP devices at version 5.0.9 or later.

Are there any complications if I've recently upgraded FortiOS?

From FortiOS 5.2.3 onward, the CLI command `auto-join-forticloud` is enabled by default, and must be enabled for FortiDeploy to function correctly.

But upgrading the FortiOS firmware from 5.0.x to 5.2.2 or later automatically disables `auto-join-forticloud`, which will need to be re-enabled or FortiDeploy will not function.

You can re-enable it through the CLI or by factory resetting your device (but factory resetting will reset all firewall configuration).

```
config system fortiguard
   get
      set auto-join-forticloud enable
   end
end
```

After changing this setting, restart the device and ensure that traffic is being sent to FortiCloud to verify that it has been configured correctly.

What if I am connected to FortiCloud but the device is not cloud-managed?

Double-check that central management is set to FortiGuard.

In the CLI console:

```
config system central-management
   set type fortiguard
end
```

Reboot the device, login to FortiCloud and try to manage the device.

What if a device is deployed behind a NAT device (such as a cable modem)?

A FortiGate's default "internal" IP is in the 192.168.1.0/24 subnet, and so IP conflicts can occur with FortiDeploy-managed devices. The solution is to unset the default IP for each of the devices in the CLI console:

```
config system interface
   edit internal
      unset ip
   end
end
```

Or change the internal interface's IP in the web-based management interface.

FortiCloud Cookbook

This series of short 'recipe' tutorials will show you how to enable and set up various FortiCloud services and features. For more in-depth explanations of individual features and functions, consult the *Frequently Asked Questions*.

Basic configuration

FortiCloud has many features available, depending on the size of your network and your interest in monitoring and management. First, devices must be added to the service.

Basic FortiCloud setup

1. Register the FortiGate/FortiWiFi on the Service and Support Portal at support.fortinet.com.
2. Create a FortiCloud account in the FortiGate/FortiWiFi dashboard licensing widget.
3. Activate the FortiGate/FortiWiFi within the dashboard licensing widget.
4. Create a firewall policy with logging enabled. Configure log uploading, if necessary.
5. Log into the portal at https://www.forticloud.com.

Adding standalone FortiAP to FortiCloud

1. Register for a FortiCloud account at https://www.forticloud.com.
2. Click the “Add Device” link and enter the unique FortiCloud key located on your FortiAP device.
3. Deploy the FortiAP to an existing AP network or create a new AP network.
4. Associate your FortiAP with an SSID.
5. Connect your FortiAP to an internet connection, and wait for it to self-configure.
6. Log into the portal at https://www.forticloud.com to configure it further.

FortiCloud Sandbox setup

1. Register the FortiGate/FortiWiFi on the Service and Support Portal at support.fortinet.com.
2. Create and activate a FortiCloud account in the FortiGate/FortiWiFi dashboard licensing widget.
3. Go to **System > Config > FortiSandbox**, and under **FortiSandbox Settings**, select **Enable Sandbox Inspection**, and select 'FortiSandbox Cloud'. The associated FortiCloud Account should appear below.
4. In **Security Profiles > AntiVirus**, create a profile that has **Send Files To FortiSandbox Cloud For Inspection** enabled.
5. Create a firewall policy with logging enabled, that uses the FortiSandbox-enabled AntiVirus profile.
6. Once some files have been uploaded to the FortiCloud Sandbox, log into the portal at https://www.forticloud.com to see the results.

FortiDeploy setup

1. Purchase a FortiDeploy SKU when you purchase your FortiCloud subscription, or by contacting cs@fortinet.com if you have already purchased a FortiCloud subscription.
2. Visit forticloud.com and enter the Bulk FortiCloud Key, you will see a list of serial numbers from the order that contained the FortiDeploy SKU.
3. Send an email to FortiDeploy Support, at cs@fortinet.com to confirm your subscription and start the service.
4. Once you confirm that the devices are connected with FortiDeploy, you can deploy basic configurations to the devices remotely.

Indicator of Compromise (IOC) setup

Note: The basic form of IOC is free, and functions for all of your FortiCloud-connected devices. In order to purchase the complete form of IOC, follow the instructions below.

1. Open the **Plan** page in the FortiCloud IOC site, and select **Buy Online**.
2. Complete the purchase process, and wait for the key to arrive by email.
3. Log into the Fortinet Support portal at http://support.fortinet.com.
4. On the Asset page, register the code as if it were a new product's serial number, and then enter the serial number of the FortiCloud-connected device that you want the service to monitor.
5. The service will automatically take effect.

FortiCloud device configuration

Whether you are creating a FortiCloud AP Network, or just monitoring multiple devices, you can use a variety of features to remotely manage and configure your networked devices.

Deploying cloud configuration to devices

1. Go to **Management > Config**.
2. Before you edit any settings, select **Import** in the upper right to retrieve the most up-to-date configuration from the FortiCloud-connected device.
3. On this page, you have limited access to an analogue of the FortiGate interface, allowing you to edit interfaces, routes, policies, etc. Edit the FortiGate configuration as needed.
4. When you are ready to push your updated configuration back to the device, select **Deploy** in the upper right.
5. Wait for the configuration to download to the device. When it completes, a Deployment Log will appear, showing you the changes as they appear in the CLI.

Device configuration backup to cloud

1. Go to **Management > Backup**.
2. Select **Backup Config** in the upper right, and enter a name for the backup revision.
3. The new configuration will be added to the list. By selecting the icons on the right side, you can rename, view, compare, download, restore, and delete configuration files. The compare icon will only appear once you have multiple revisions available.

Remote device firmware upgrade

1. Go to **Management > Upgrade**.
2. Verify your device's current firmware version in the upper left before continuing.
3. If you are concerned about the effects of upgrading or have not upgraded recently, please read the FortiOS Upgrade Path document, available at http://docs.fortinet.com.
4. We also recommend that you back up your device's configuration before upgrading, either in **Management > Backup** or in the device's management interface.
5. Select an Available Firmware from the list that you would like to upgrade the device to, and select **Upgrade**.
6. Wait for the upgrade to take effect.

Remote device script execution

The Script deployment functionality allows you to upload scripts and run them as needed on a schedule basis.

1. Go to **Management > Script**.
2. In the upper right, select **Add Script**.
3. Enter a name and a description, and the content of the CLI script that you want to run. Save the script.
4. On the right, select **Schedule Deployment** icon, and select a time that you'd like the script to be automatically deployed to the device.
5. If you need to cancel the scheduled run, select the blue arrow next to the scheduled time.

Advanced configuration

Some features of FortiCloud are more useful for larger/more distributed networks: more refined oversight, multiple administrators, multiple regions, or other complex setups.

Adding more administrators/users

1. In the upper right of the FortiCloud interface, select the **My Account** icon.
2. Select **Add User** in the window.
3. Enter the email address and name of the new user/admin.
4. Select whether they are an Admin (total control over the FortiCloud interface) or a User (limited control, monitoring only).
5. Select **Submit**. They will receive an email prompting them to set their account password, and log in.

Creating custom FortiCloud reports

1. Go to **Analysis > Reports**.
2. Select **Add** in the upper right, and choose whether to create a new report, edit an existing template, or import an external template.
3. Select the gear icon on the right side to add Charts and Headers to the current section, or new 1- or 2-column sections.

4. Edit charts by selecting the pencil icon in the upper right of each chart, and selecting a predefined chart style or setting the axis variables manually.
5. When you're finished, select **Save** in the upper right.
6. Select **Run**, and view the finished report.

Configuring FortiSandbox alert emails

1. Go to **Sandbox > Setting**.
2. Select **Enable Alert Setting**.
3. Enter emails into the list that should be contacted in the event of a FortiSandbox Alert.
4. Select the levels of severity that will trigger an Alert.

FortiCloud Multi-Tenancy configuration

A Multi-Tenancy Account is a subscription account that allows you to create and manage multiple sub-accounts that are functionally isolated from each other. Devices can be added to and moved between these sub-accounts, and each account can have its own administrators and user s.

Activating Multi-Tenancy feature

1. Contact your Fortinet Partner or Reseller, requesting the following SKU: “FCLE-10-FCLD0-161-02-DD”.
2. You will receive a Multi-Tenancy Activation Code from them by email.
3. Open the FortiCloud interface, and select the **My Account** icon in the upper right.
4. Under the admin/user list, select **Activate Multi-Tenancy Feature**.
5. Enter the Activation Code, and **Submit**.

Basic Multi-Tenancy configuration

Once Multi-Tenancy has been activated, the default FortiCloud Home page will be replaced with the Multi-Tenancy page, which has 'FortiGate', 'AP Network', and 'Inventory' at the top.

1. Open the **Inventory** page, and select **Import Key** from the upper right, either **FGT**, **AP**, or **Bulk** if you want to add multiple FortiCloud licenses at once.
2. Import all the dev ices and/or licenses you like. They will be listed under **FortiGate Inventory**, and **AP Inventory**.
3. On an Inventory subpage, select a device, and select **Deploy** in the upper right to assign it a license. It will be automatically moved to the **Deployed FortiGates**/**APs** subpage.
4. Select either **FortiGate** or **AP Network** from the top, and select a device to individually configure it further.